RSAC 2025 Conference

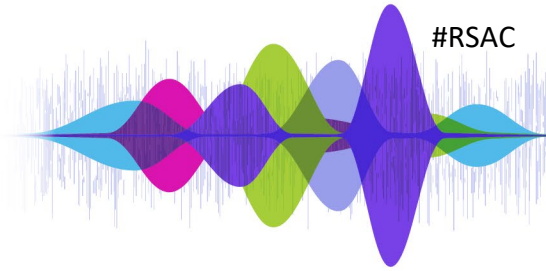
Many Voices.
One Community.

SESSION ID: PART4-T09

DLP for Today's Threat Landscape

Brian Vecci

Field CTO
Varonis
https://www.linkedin.com/in/brianvecci/



Disclaimer

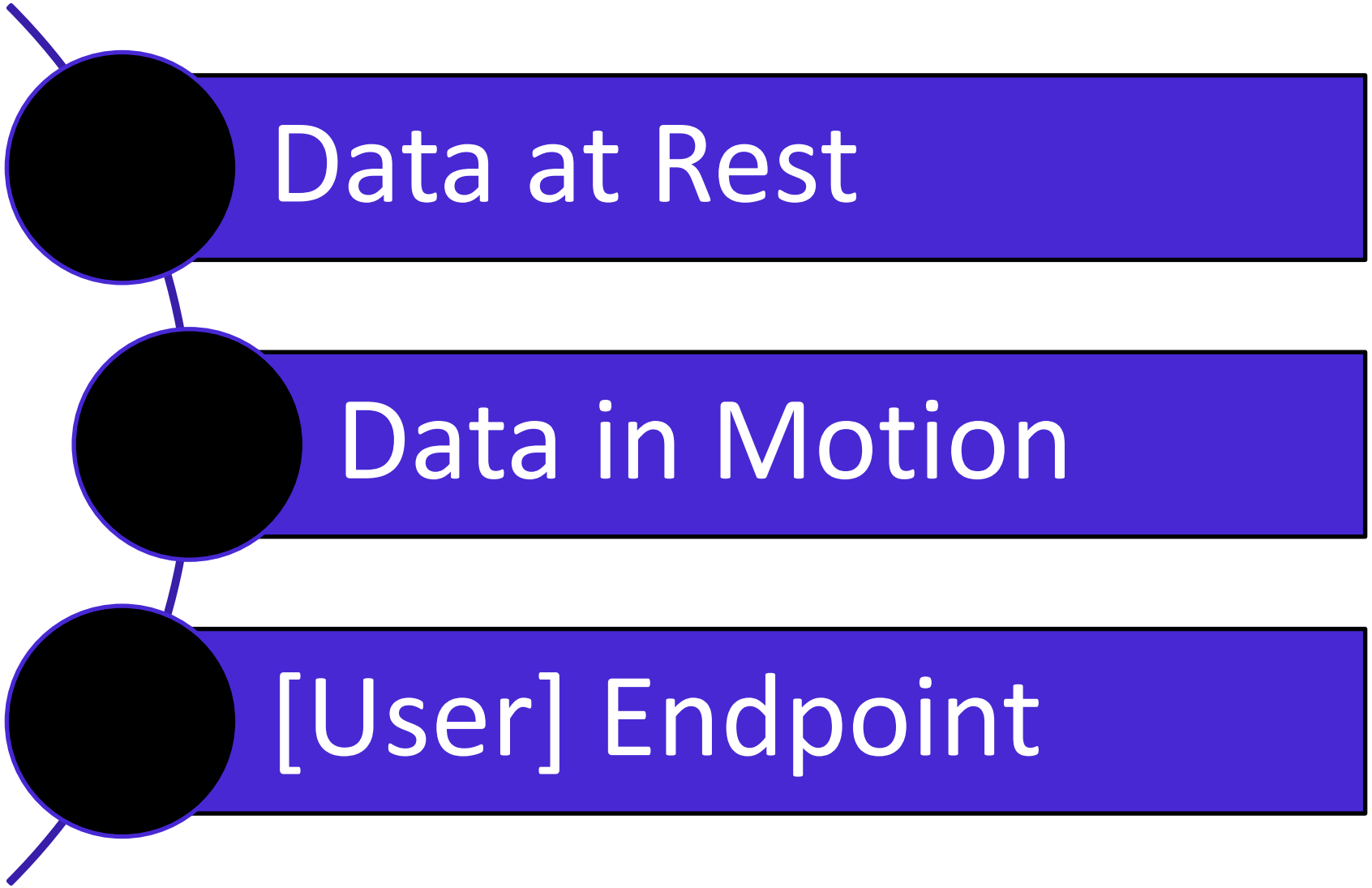
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

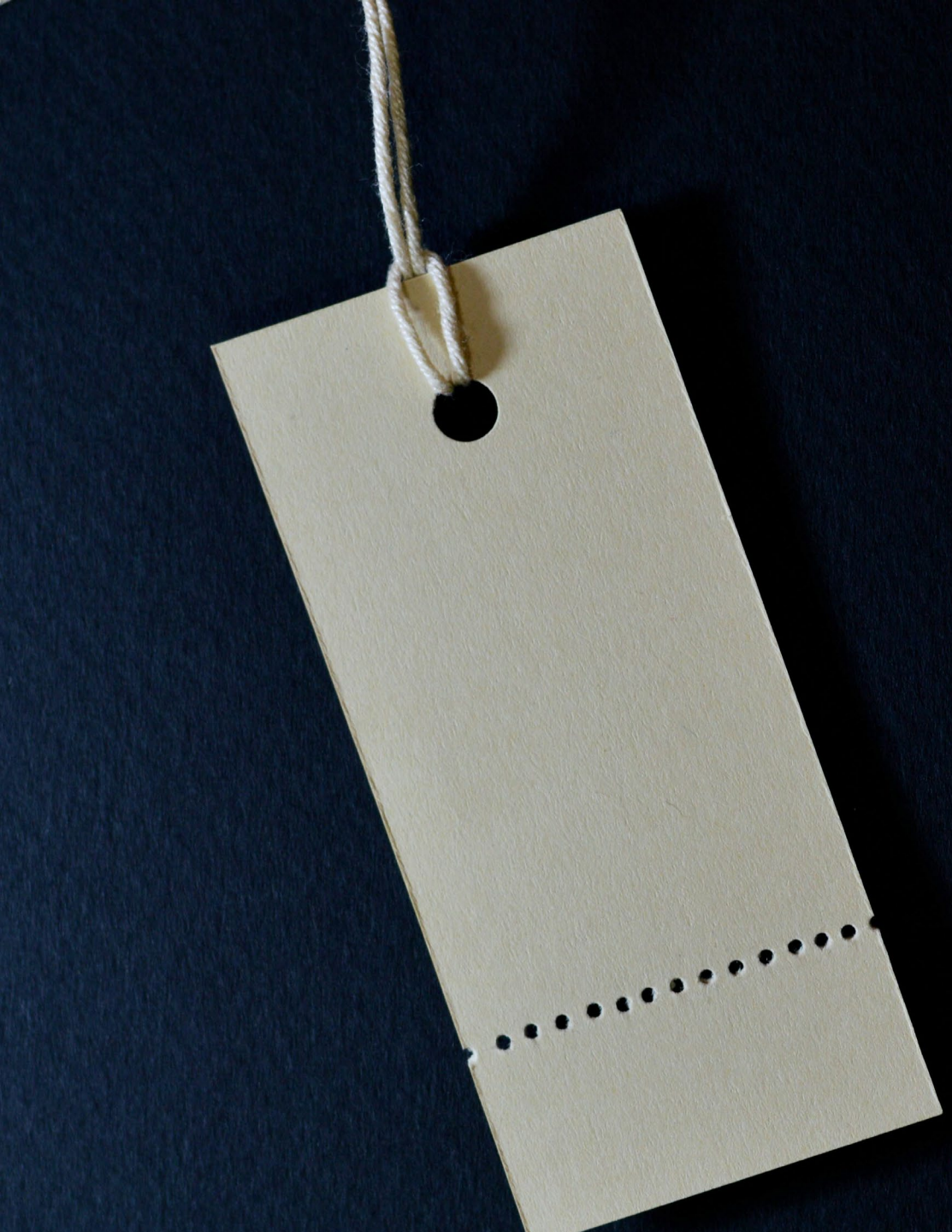
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Data loss protection (DLP) *describes a set of technologies and inspection techniques used to* ***classify information content*** *contained within an object — such as a file, email, packet, application or data store — while at rest (in storage), in use (during an operation) or in transit (across a network). DLP tools are also have the ability to* ***dynamically apply a policy*** *— such as log, report, classify, relocate, tag and encrypt — and/or apply enterprise data rights management protections.*

What's DLP?


Data at Rest
Data in Motion
[User] Endpoint



What about labels?

So DLP prevents the loss of data?

Data is where the damage happens.

Amazon Confirms Employee Data Was Exposed Through MOVEit Breach
Hackers may have stolen the Social Security numbers of every American. Here's how to protect yourself
Yet another ransomware attack - an NHS children's hospital is the latest victim
News
By Ellen Jennings-Trace published 13 hours ago
Alder Hey Children's Hospital is reportedly exploring data breach
CNN Politics
SCOTUS
Congress
Facts First
2024 Elections
Iranian hackers sent stolen Trump campaign information to people associated with Biden campaign

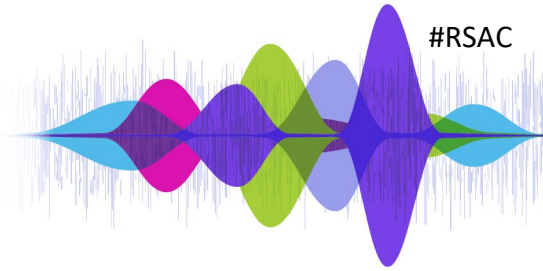
CISOs want to do four things…

Stop Breaches

Prove They're Compliant

Automate

Prove they did it



Why DLP Fails

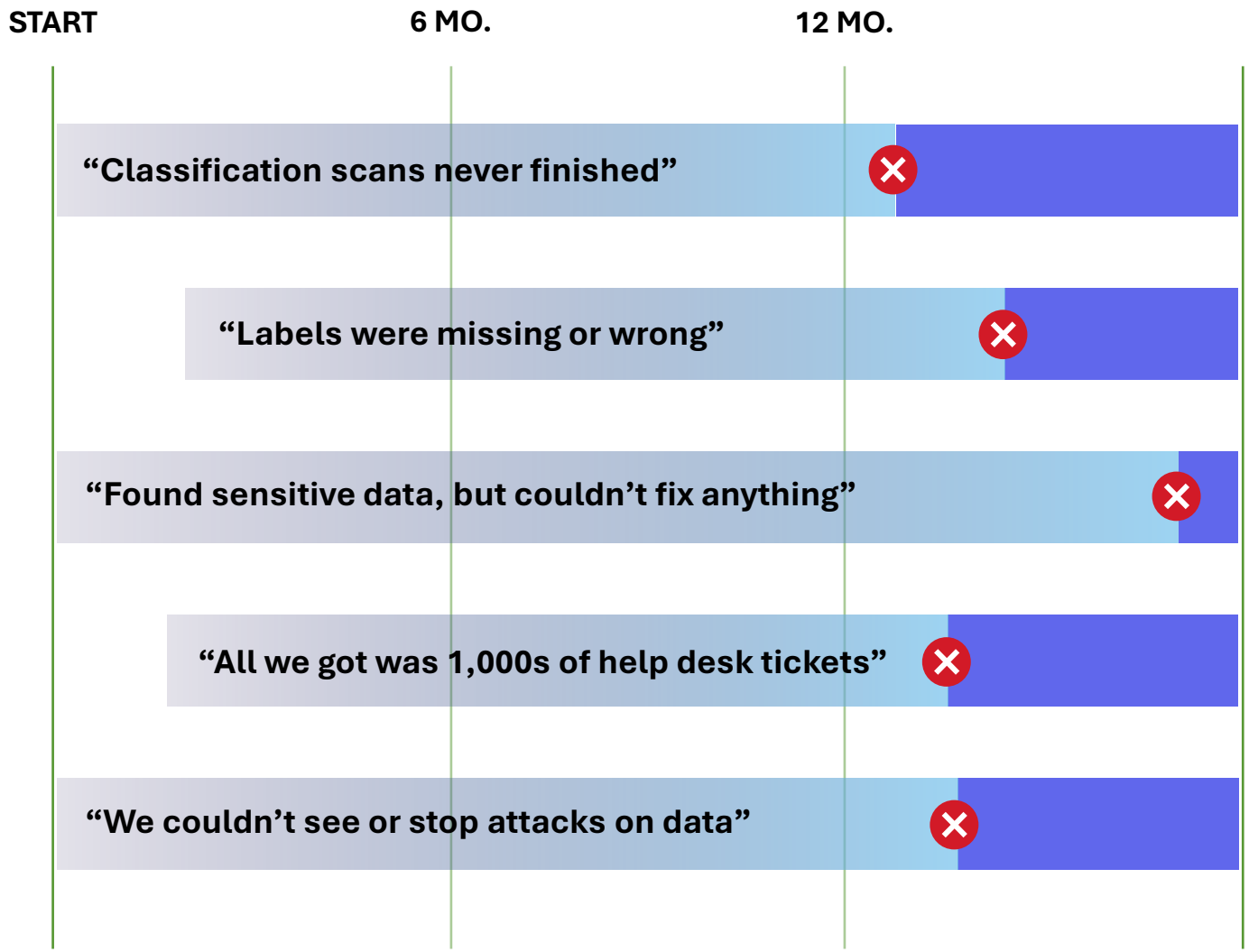
- Where’s all the data?
- Who’s putting it there and why?
- Is all of it labeled? Accurately?
- Who (and what) has access to what?
- Can a perimeter control stop an insider?

Time
15m
1H
4H
1D
1W
2021/04/15 10:30 O: 22.983 H: 22.983 L: 22.983 C: 22.981 CHANGE: 0.01% AMPLITUDE: 0.00%
MA(7): 23.087 MA(25): 23.226 MA(99): 23.238
23.899
22.403

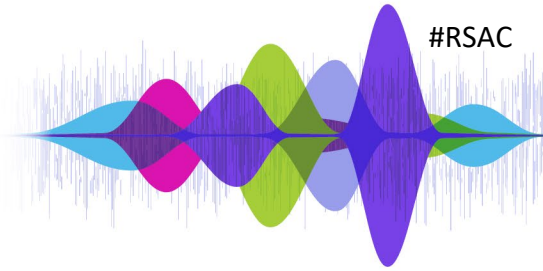
Most solutions result in busywork followed by a breach.

We spent 18 months struggling just to classify data with **no measurable outcome.”**

CISO, Global Financial Firm


START
6 MO.
12 MO.
“Classification scans never finished”
“Labels were missing or wrong”
“Found sensitive data, but couldn’t fix anything”
“All we got was 1,000s of help desk tickets”
“We couldn’t see or stop attacks on data”

Attackers don’t break in, they log in.

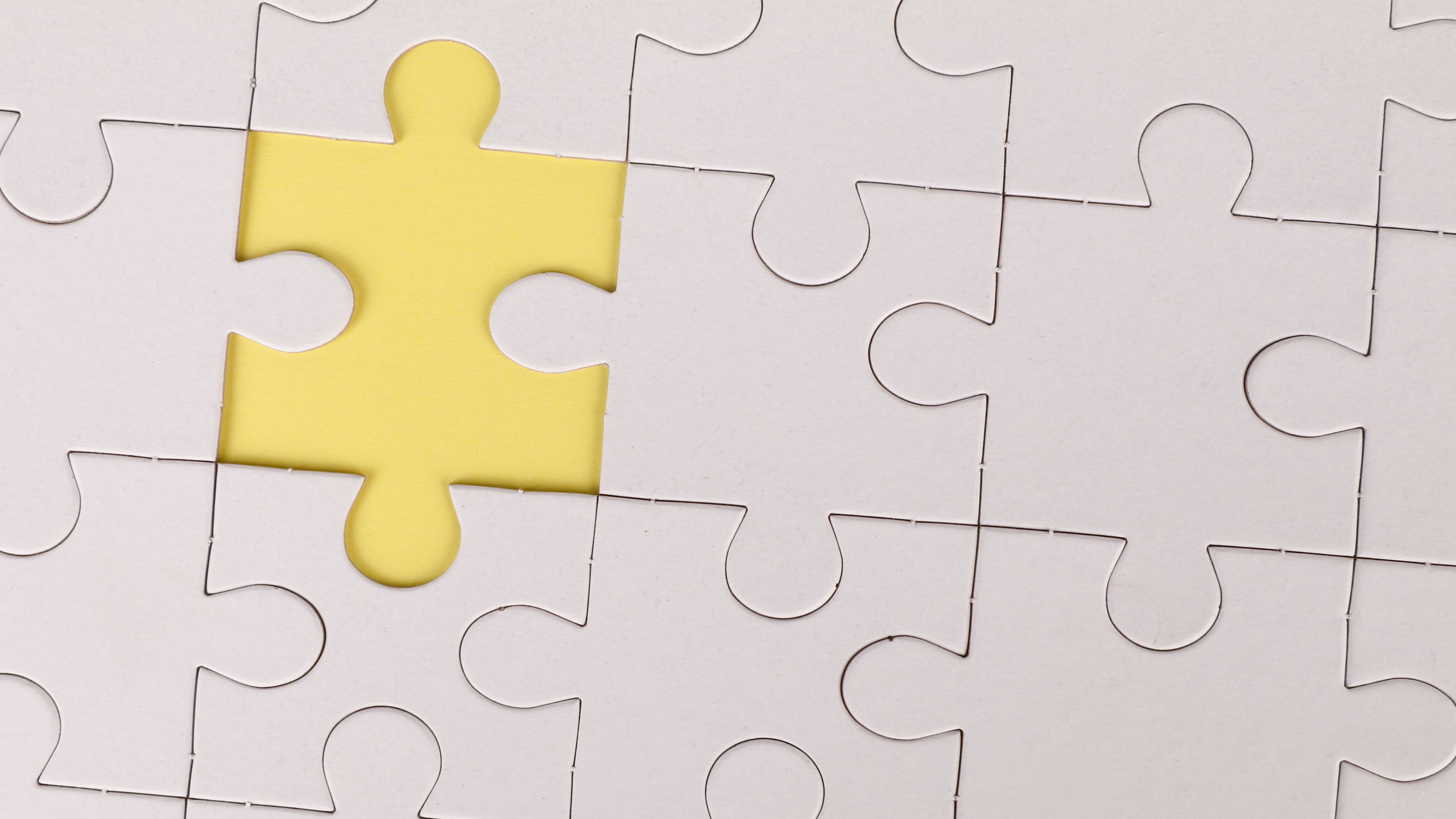


What's needed for modern DLP?

- Data classification & accurate labels
- Effecting posture management
- Least privilege access
- All kinds of telemetry
  - Data access
  - Sharing
  - Config & Posture Change
  - Data flows

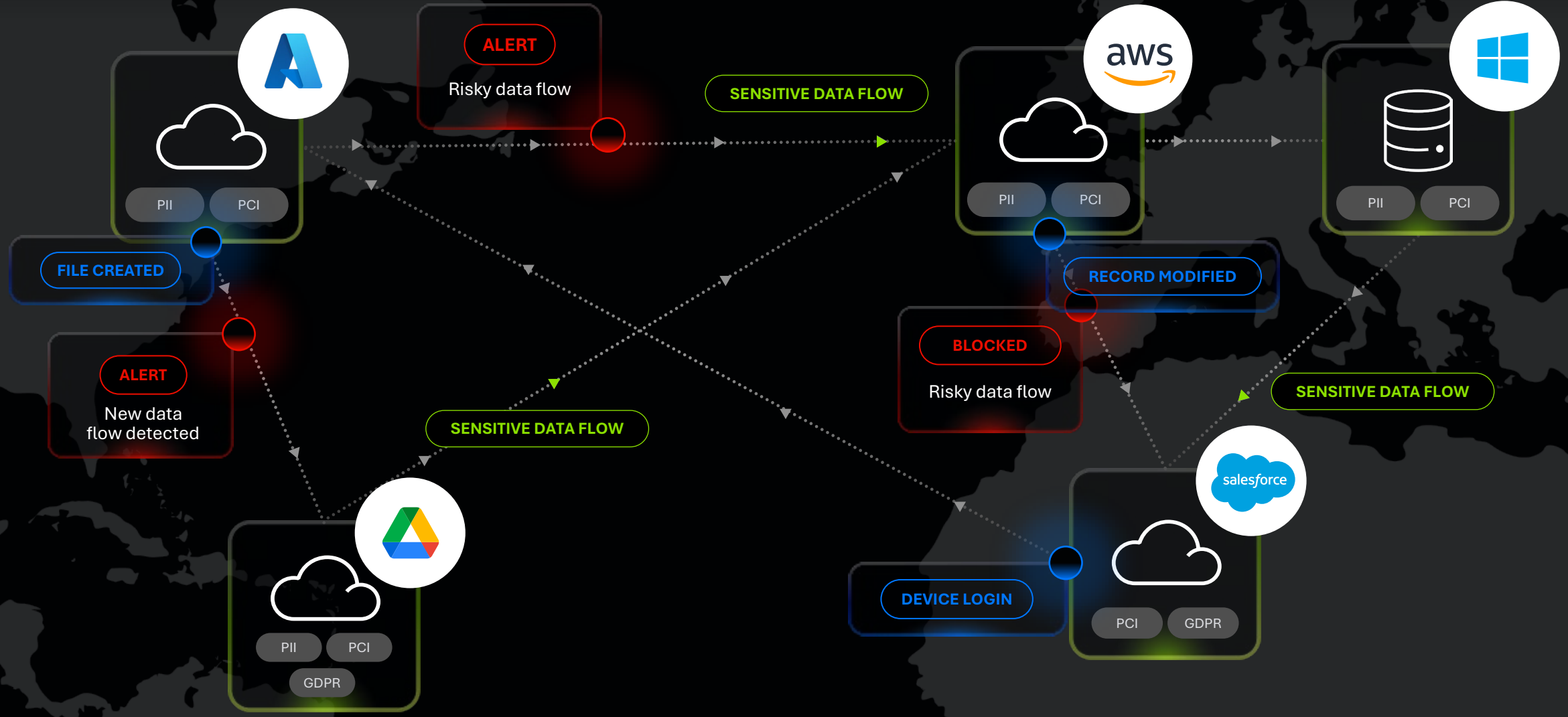
And then you must put it all together.

Context is everything.

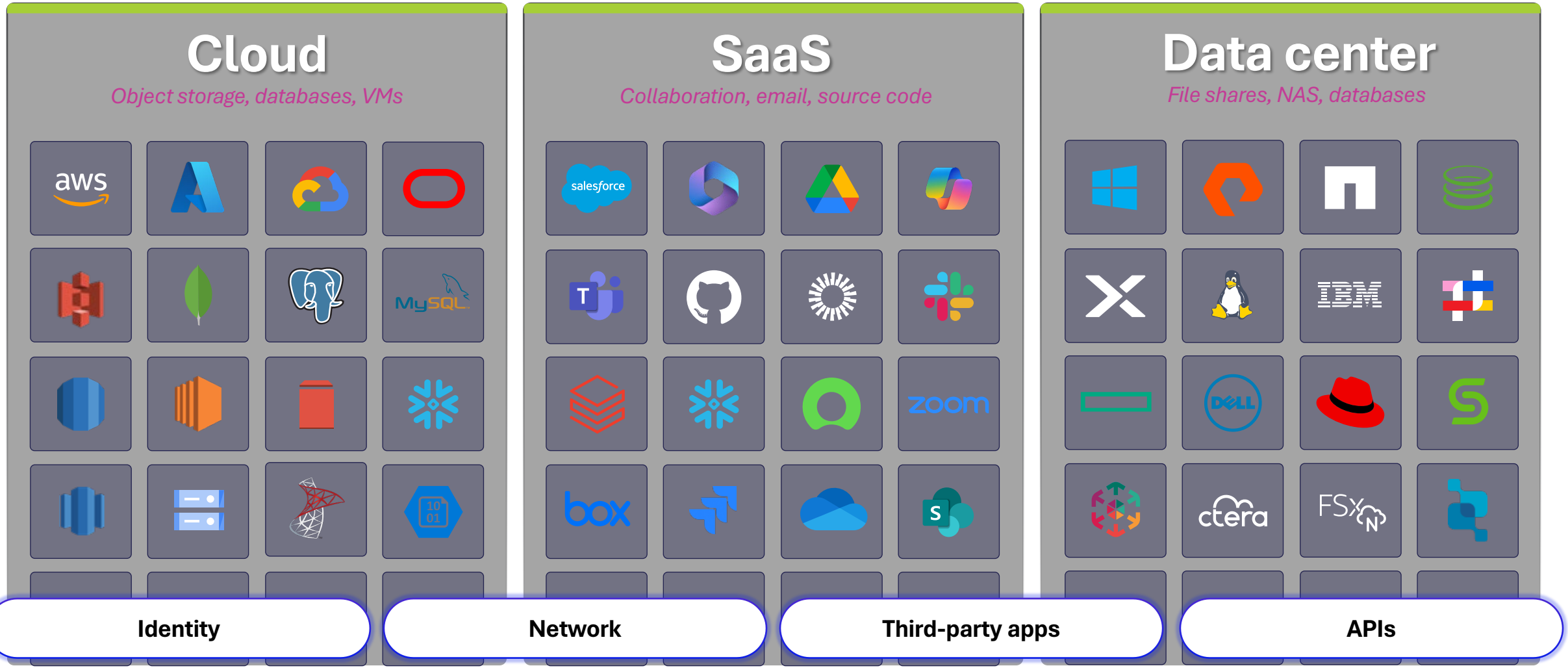


RESULT

Next-Gen DLP


ALERT
Risky data flow
SENSITIVE DATA FLOW
PII
PCI
FILE CREATED
ALERT
New data flow detected
SENSITIVE DATA FLOW
PII
PCI
GDPR
aws
PII
PCI
RECORD MODIFIED
BLOCKED
Risky data flow
DEVICE LOGIN
PII
PCI
SENSITIVE DATA FLOW
salesforce
PCI
GDPR

Data Lives Everywhere



Provable Compliance in 10 days

Automation reduced a healthcare system's Copilot exposure by 99.8% in 10 days.
Zero impact on the business using 20 automation policies to lock down ~1 million files.

992K
files

Starting point

~1M files across the org's SharePoint, Teams, and OneDrive. Varonis quickly classified 120K sensitive files.

57K
exposed files

Identifying Copilot risk

Identify exposed PHI, PII, credentials at risk of being exposed via Copilot.

99.8%
exposure reduction

10-Day Difference

Automatically eliminated ~2K sharing links and right-sized access to 57K files with automatic policies.

0
tickets complaints

Zero customer impact

Proactively notified M365 admins of the remediation plan. The team heard zero complaints.

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

Varonis

RSAC Booth: N-5658